Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 1684 – 1691

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Image Watermarking using Diffie Hellman Key Exchange Algorithm

Aparna J R[a], Sonal Ayyappan[b]*

[a]*Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, Kerala, India*
bDepartment of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, Kerala, India

Abstract

Digital watermarking is the method of hiding or embedding any form of digital data in another multimedia data like image, audio, video, text, etc. The image to which another image is hidden is the cover image or original image and the hidden image is known as watermark. This paper proposes a block based image watermarking algorithm which uses cryptographic algorithm to find out the positions of the cover image in which the watermark is to be embedded. Two different keys are generated using Diffie Hellman Key Exchange algorithm and using these keys the positions of cover image to which the watermark bits are to be embedded are found out. Experimental results show that this method can withstand different geometrical attacks and is robust than other methods.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

*Keywords:*Watermark;Cryptography; Key; Diffie Hellman; Block; Robust

1. Introduction

The process of hiding or embedding one digital data in any other multimedia data such as image, audio, video, etc[12, 13] is called digital watermarking. The embedded data can be visible or invisible to the users. Digital image watermarking was developed as a variation of steganography, which is a method of hiding a secret message

* Aparna J R. Tel.:+91-9496258131.
*E-mail address:*aparnajr31@gmail.com

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.02.109

in another message. In earlier days, watermarks were used as logos to assert ownership of a company on its product. Photographers use their logo or signature as watermark and embed it in their photograph to indicate ownership. Watermarks are now widely used for copyright protection of multimedia data (in currencies, paper and postage stamps) in order to avoid fraud and forgery. Digital watermarking has wide range of applications[11, 19] in many areas such as computer science, cryptography, signal processing and communications.

The increased use of Internet has made easier transmission of multimedia data. But these data may get affected by any unwanted noise in the channel. Some third party can also attack the data or deliberately try to tamper the data. For secure transmission, the sender can embed the original image with any logo or image. The embedded data is called the watermark. The receiver extracts the hidden watermark from the watermarked image using the same technique which was used for embedding the watermark. Distortions in the extracted watermark help the receiver to identify that the image has been attacked at the channel.

Image Watermarking techniques are mainly categorized into two - (a) spatial domain and (b) frequency domain techniques. The frequency domain techniques are found to be more robust when compared to spatial domain techniques[6, 10]. Discrete Wavelet Transform (DWT)[10], Discrete Cosine Transform (DCT)[17], Discrete Fourier Transform (DFT)[14], etc are various transform domain techniques. Block based watermarking is another relevant watermarking technique which divides the image into different blocks and the watermark is embedded in these blocks. Embedding capacity is increased with the number of blocks in the cover image. This method is more robust and efficient compared to non-block based watermarking techniques. Different methods are introduced to attack the watermarked images at transmission time. So, it is a difficult task to find out the best watermarking method. The challenge of the attacker is to obtain the embedding bits of the cover image. If the owner randomly chooses the embedding bits, it will be difficult for the attacker to find out the bits. So new methods can be used to find out the positions of the cover image to which the watermark bits are to be embedded.

The proposed method uses the keys generated from Diffie Hellman Key exchange algorithm to find the positions of the cover image to which the watermark bits are to be embedded. The embedding is done after block dividing the cover image and the watermark image. The paper is organized as follows: Section 2 covers the related works in block based watermarking and various cryptographic techniques for watermarking in digital images. The proposed watermarking method is explained in section 3. Section 4 shows experimental results after applying attacks on the image and Section 5 gives the conclusion drawn from the analysis.

2. Related Works

Mohammad-Reza Keyvanpour[8] proposed a block based watermarking technique, which uses Discrete Wavelet Transform (DWT) to embed the watermark into the cover image. The method uses dynamic blocking for choosing the positions to which the watermark bits are to be embedded. The pixels in HL and LH sub bands of the DWT transformed image is selected for dynamic blocking since they are related to strong edges. The method is robust compared to other non-block based methods and highly suitable for maps and local images.

Anand Kunwar Singh[7] has proposed a block based watermarking technique which uses histogram shifting. In this, the block number is increased in order to improve the embedding capacity. The image is divided into 16 equal blocks and histogram of each block is considered. From this histogram, the watermark embedding bits are found out. The algorithm increases the capacity and keeps the signal to noise ratio constant.

Lin Gao[3] proposed a new reversible watermarking technique, which is based on Integer Discrete Cosine Transform (IntDCT) and Difference Expansion (DE). The image is first divided into non-overlapping blocks. The blocks with energy less than some predefined threshold is selected and the difference expansion embedding is done on them. This algorithm has effective applications in medical image processing.

Y.F.Chang[2] proposed a block-based watermarking technique for tamper detection and self-recovery of images. The watermark is embedded into image blocks. The method uses parity check and intensity-relation check to prevent malicious attacks. To evaluate the legitimacy of each block, the block neighborhood is taken into account. The method can resist collage attack, vector quantization (VQ) attack and constant average attack.

Watermarking techniques were combined with cryptographic methods to provide security of the images. Shu-Fen Tu[9] proposed a watermarking method which employs visual cryptography. Here, a binary image is used as the watermark. The watermark image is then divided into two parts, one part is embedded into the original image

and the other part is kept by the owner. To ensure ownership, the owner has to extract one part from the image and recover with his own share.

Watermarking algorithm with Data Encryption Standard (DES) was proposed N.Tiwari[1]. Here, the watermark is encrypted using DES algorithm and embedded in the DWT domain. The original image is subjected to two level DWT in order to ensure robustness. The watermark is DES encrypted with a key. To extract the watermark image the secret key is needed.

Bouslimi D[4] proposed a method that combine encryption and watermarking techniques for secure image transfer. This method combines watermarking, public-private keys and secret keys and encryption algorithms. A secret key is used in this method and is encrypted using an asymmetric algorithm. This encrypted key is inserted into the encrypted image by using watermarking algorithm.

The cryptographic functions are used for encrypting the watermark information or to encrypt the secret key used for watermarking. But, the selection of embedding bits from the original image is not much considered in the above methods. The cryptographic algorithms can be used to compute values and the watermark can be embedded in the original image with the help of these values, so that it will be difficult for the attacker to find out where the watermark was embedded.

3. Proposed Method

In most of the watermarking algorithms, the bits of the watermark are embedded directly on the cover image. This will make the task of the attacker easier to find out the positions where the watermark is present. So the positions are to be selected randomly in order to provide security. In the proposed method the help of cryptographic algorithm is used to find out the positions. The positions in the cover image to which the watermark bits is to be embedded is found out by using Diffie Hellman Key Exchange algorithm. First of all, two keys are generated and using that key, the locations to embed are found out.

3.1. Watermark Embedding

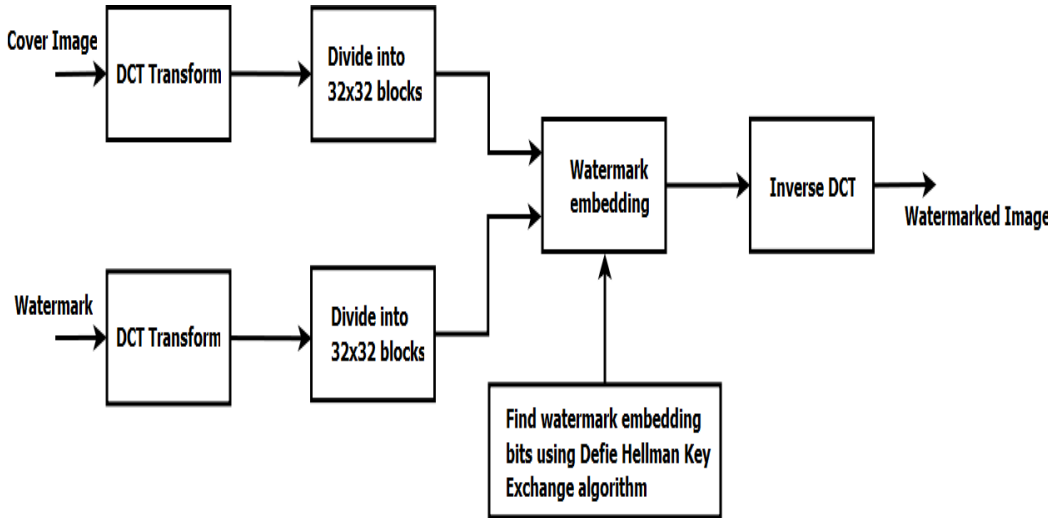


Fig. 1. Watermark embedding

The watermark embedding process is shown in Fig. 1. The cover image and the watermark are converted into frequency domain by performing DCT conversion. Then, the resultant image is divided into 32x32 blocks. Then, two keys are generated using Diffie Hellman key exchange algorithm to find out the *(x, y)* position to which

the watermark bits are to be embedded. The steps of key generation are explained below.

- The algorithm requires two large numbers, one prime (n), and (g), a primitive root of n
- Then, select any two private values a and b.
- Compute public values x' and y'.
  - $x' = g^a \bmod n$
  - $y' = g^b \bmod n$
- Public values x' and y' are exchanged
- Compute shared, private key
  - $k_a = y^a \bmod n$
  - $k_b = x^b \bmod n$
- Algebraically, we can prove that $k_a = k_b$

This is Diffie Hellman key exchange algorithm.

In the proposed method, two keys k_1 and k_2 are generated from two different n and g. The cover image is divided into non-overlapping image blocks each of size 32x32. The steps of watermark embedding are explained below.

- Take a value $p=1024$ (Since the number of pixels in each block is 1024).
- Find the 32 positions of watermark embedding bits
- Compute $mod(p,k_1)$.
- If it is greater than 32, decrement 32 from the value.
- Next value is computed by taking $mod(p-1, k_1)$.
- Thus, the x values of pixel positions are computed.
- Similarly, find the value of y using k_2 .
- Embed the watermark bits in the (x , y) position of the block.

The watermark bits are embedded in the cover image using the equation (1).

$$WI = I + k * W \tag{1}$$

Where, WI is the watermarked image, I is the original cover image, W is the watermark and k is the strength factor.

3.2. Watermark Extraction

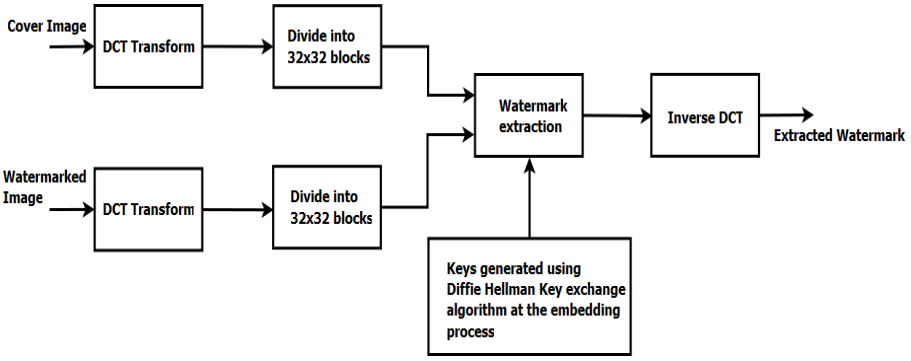


Fig 2. Watermark extraction

The original image and the watermarked image are input for watermark extraction. Also, the keys k_1 and k_2 are also given for extraction. With the help of the cover image and the keys, the watermark image is extracted from the watermarked image. The block diagram of watermark extraction is given in Fig 2.

The cover image and the watermarked image are converted into DCT domain and then divided into 32x32 blocks. The same procedure of embedding is also done in extraction using the keys k_1 and k_2 in order to find out the positions where watermark is present. The watermark is extracted using (2).

$$W' = (WI - I)/k \tag{2}$$

Where, W' is the extracted watermark.

4. Experiments and Results

4.1. Experimental set up

The proposed watermarking algorithm was experimented on 3 different cover images and different types of watermarks where used. The types of images used are constant colored images, diverse colored images, logos and complex shaped polygon images. Examples of each type are shown in Fig. 3. The experiment was conducted in MATLAB.

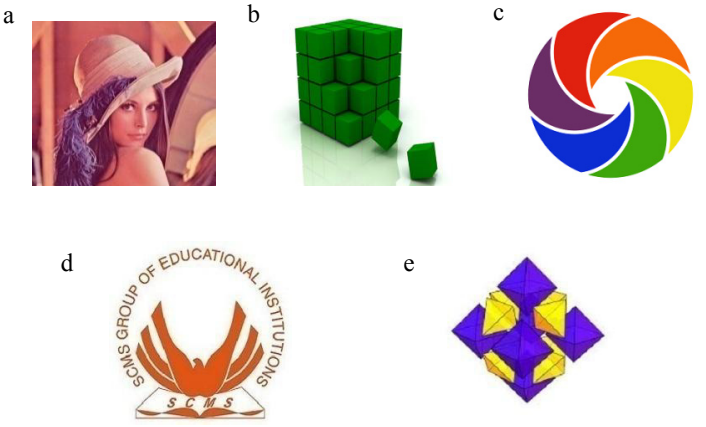


Fig. 3. (a) Cover image; (b) Constant colored watermark; (c) Watermark with diverse colors; (d) Logo watermark; (e) Complex polygon shaped watermark.

4.2. Evaluation Parameters

In order to evaluate how much robust the proposed method is, the watermarked image is subjected to different types of attacks[15]. The attacks applied are Scaling, Blurring, Sharpening and Salt-and-Pepper noise. Then, the Peak Signal to Noise Ratio (PSNR)[5, 18], Normalized Correlation (NC)[10, 13] and Similarity Index (SI)[10] values of the extracted watermark with respect to the original watermark are calculated.

Peak Signal-to-Noise Ratio (PSNR): Peak Signal to Noise Ratio (PSNR) is computed to analyze the concealing effect of the watermark. It is calculated as the ratio between the maximum power of the original image and the

power of unwanted noise which is added to the image (which will affect the exactness of its representation). The formula to find out PSNR is shown in (3).

$$PSNR = 10\log_{10}\frac{M^2}{\frac{1}{m\times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2} \tag{3}$$

Where, M is the power of the signal, $I(i,j)$ is the original watermark and $K(i,j)$ is the extracted watermark. Bigger the PSNR value better the watermark conceals.

Normalized Correlation (NC): The robustness of the proposed algorithm is analyzed by using Normalized Cross Correlation (NC). It is a metric to evaluate the degree of similarity (or dissimilarity) between two compared images. The original watermark and the extracted watermark are compared. The equation to compute NC is given in (4).

$$NC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W(i,j)]^2}\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W'(i,j)]^2}} \tag{4}$$

Where, $W(i,j)$ is the original watermark and $W'(i,j)$ is the extracted watermark. The value of NC is between 0 and 1. As the value increases, the method will be more robust.

Structural Similarity Index (SI): It is an equation for measuring the similarity between two images. Structural Similarity Index can be considered as a quality measure of an image. That image is compared with another image which is considered as perfect quality image. The equation to find out similarity index values is shown in (5).

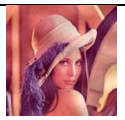
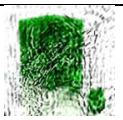
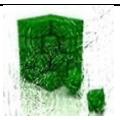
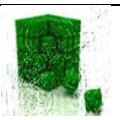
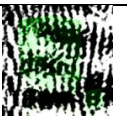
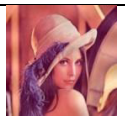
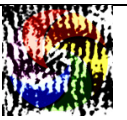
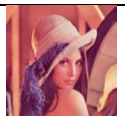
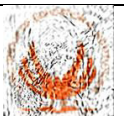
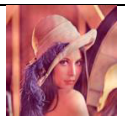
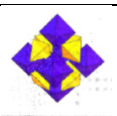
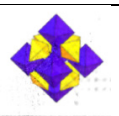
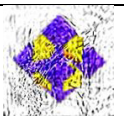
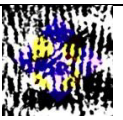
$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{5}$$

Where μ_x is the average of x, μ_y is the average of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y; σ_{xy} is the covariance of x and y; $c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$, which are the two variables to stabilize the division; L is the dynamic range of pixel values and $k_1 = 0.01$ and $k_2 = 0.03$.

4.2. Results

Different attacks are applied on the watermarked image for evaluating the robustness of the proposed method. The attacks applied are Scaling, Blurring, Sharpening and Noise. Then, the watermark is extracted and the extracted watermark is compared with the original watermark using the evaluation parameters mentioned above. The results of "lena.jpg " with different kinds of watermark is given in Table I.

Table 1. Results of watermarking using Diffie Hellman Key Exchange

Watermarked Image	Extracted Watermark				
	No attack	Scaling	Blurring	Sharpening	Noise
	 PSNR=64.13, NC=0.99,SI=0.99	 PSNR=63.88, NC=0.99,SI=0.99	 PSNR=30.03, NC=0.77,SI=0.7	 PSNR=46.36, NC=0.95,SI=0.95	 PSNR=11.43, NC=0.04,SI=0.04
	 PSNR=62.64, NC=0.95,SI=0.95	 PSNR=62.36, NC=0.95,SI=0.95	 PSNR=29.36, NC=0.46,SI=0.36	 PSNR=43.48, NC=0.74,SI=0.73	 PSNR=16.16, NC=0.02,SI=0.02
	 PSNR=49.29, NC=0.92,SI=0.91	 PSNR=49.17, NC=0.92, SI=0.91	 PSNR=28.84, NC=0.49, SI=0.49	 PSNR=41.79, NC=0.82, SI=0.81	 PSNR=10.23, NC=0.02, SI=0.02
	 PSNR=62.64, NC=0.99, SI=0.99	 PSNR=62.33, NC=0.98, SI=0.98	 PSNR=30.08, NC=0.72, SI=0.72	 PSNR=47.19, NC=0.95, SI=0.95	 PSNR=10.74, NC=0.08, SI=0.07s

4.3. Inference

From Table I, the PSNR values are relatively high when there is no attack in the watermarked image. Also, the NC and SI values are near to 1, which shows the method is robust enough and conceals better. After applying attacks, the PSNR values are not much reduced. The table shows that the proposed method is more robust against scaling attacks and more affected by Salt-and-pepper noise attack (since the PSNR, NC and SI values are comparatively less). Similar trends are seen in all the test images which were used for watermarking using the proposed method. But, due to lack of space results of "lena.jpg" image are only shown in the Table 1.

5. Conclusion

The paper presents a block based watermarking technique in which cryptographic algorithms are used to find out the positions in the cover image to which watermark has to be embedded. The cover image and the watermark are transformed into frequency domain using Discrete Cosine Transform (DCT) and divided into 8x8

blocks. The watermark embedding bits of each block are found out by using the keys generated by Diffie Hellman Key Exchange algorithm. With the help of the keys, 32 random positions of each block of the cover image is found out. Thus, the watermark is embedded in each block of cover image. The experimental results show that the proposed method is robust enough to withstand scaling, blurring and sharpening attacks. The watermark is less affected by scaling attack and is more affected by noise attack. The high PSNR, NC and SI values proves that the method is robust than other methods also.

References

1. Tiwari N., Kumar Ramaiya M, Sharma M., Digital Watermarking using DWT and DES, IEEEs 3rd International Conference on Advance Computing (IACC), pp. 1100-1102, Feb. 2013.
2. Y.F.Chang, W.L.Tai, A block-based watermarking scheme for image tamper detection and self-recovery, Opto-Electronics Review, volume 21, pp. 182-190, June 2013.
3. Lin Gao, Tiegang Gao, Guorui Sheng, A new reversible watermarking scheme based on integer DCT for Medical images, IEEEs International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR), 2012.
4. Bouslimi D, Coatrieux G, Cozic M, Roux C, A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images, IEEE Transactions on Information Technology in Biomedicine, Volume:16, Issue: 5, Sept. 2012.
5. N. Naveen Kumar, Dr.S.Ramakrishna, An Impressive Method to Get Better Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE) Values Using Stationary Wavelet Transform (SWT), Global Journal of Computer Science and Technology Graphics & Vision, Volume 12, Issue 12, Version 1.0, 2012.
6. Darshana Mistry, Comparison of Digital Watermarking methods, International Journal on Computer Science and Engineering, Vol. 02, No. 09, 2010, 2905-2909
7. Anand Kunwar Singh, Prasanna Kumar Acharya, Basant Kumar, High Capacity Digital Image Watermarking with Increased Number of Blocks, Proceedings of the 2011 International Conference on Communication, Computing and Security, Pages 331-334, ACM, New York, USA, 2011.
8. Mohammad-Reza Keyvanpour, Farnoosh Merrikh-Bayat, Robust Dynamic Block Based Image Watermarking in DWT Domain, Procedia Computer science, pp.238242, 2011.
9. Shu-Fen Tu, Ching-Sheng Hsu, Digital Watermarking Method Based on Image Size Invariant Visual Cryptographic Scheme, Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, pp 362-366, IEEE Computer SocietyWashington, DC, USA 2009.
10. Mei Jiansheng, Li Sukang, Tan Xiaomei, A Digital Watermarking Algorithm Based on DCT and DWT, Proceedings of the International Symposium on Web Information Systems and Applications, 2009, pp. 104-107.
11. Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering, 2006. 4, 3: 275-290
12. Francois Cayre, Caroline Fontaine, Teddy Furon, Watermarking Security: Theory and Practice, IEEE Transactions on Signal Processing, Vol. 53, No. 10, 2005
13. Du-Ming Tsai, Fast Normalized Cross Correlation for Defect Detection, November 2003.
14. J. Jiang and A. Armstrong, A Data Hiding Approach for Efficient Image Indexing, IEEE Transaction, November 2002
15. Joachim J. Eggers, Jonathan K. Su, Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks, IEEE 2001
16. Saraju P. Mohanty, Digital Watermarking : A Tutorial Review, 1999
17. Andrew B. Watson, Image Compression Using the Discrete Cosine Transform, Mathematica Journal, 4(1), 1994, pp. 81-88
18. Lin Zhang, Xuanqin Mou, FSIM: A Feature Similarity Index for Image Quality Assessment
19. Lin Liu, A Survey of Digital Watermarking Technologies